CLAIMS

1. A method of validating a message encoded according to a network protocol, the message including a plurality of subcomponents arranged in a hierarchy, the method comprising:

receiving the message at a node in a network, wherein the network is operative to communicate via the protocol;

recursively validating each subcomponent of the plurality of subcomponents, recursively validating each subcomponent further including

determining an aging limit for each of the plurality of subcomponents,

determining a sequential identifier for each of the plurality of subcomponents,

determining a wrap-around count for the subcomponent, and

for each of the plurality of subcomponents, comparing the sequential identifier to wrap count for the subcomponent, and the aging limit to a current time.

2. The method of claim 1, further comprising:

if, for a subcomponent of the plurality of subcomponents, the current time exceeds the aging limit and the if the sequential identifier is less than the wrap count, flagging the subcomponent as exceeding the age limit.

3. The method of claim 2, further comprising:

upon flagging the subcomponent, indicating the flagging to a security daemon of the network protocol.

4. The method of claim 1, further comprising:

determining if the subcomponent has been retransmitted.

5. The method of claim 1, wherein the network protocol is a routing protocol.

6. The method of claim 5, wherein the routing protocol is an Exterior Gateway Protocol (EGP).

7. The method of claim 6, wherein the EGP is a path vector protocol.

8. The method of claim 7, wherein the path vector protocol is a version of Border Gateway Protocol.

9. The method of claim 5, wherein the routing protocol is a link state protocol.

10. The method of claim 9, wherein the link state protocol is Open Shortest Path First (OSPF).

11. The method of claim 9, wherein the link state protocol is IS-IS.

12. A method of processing a network component at a first node in an inter-network, the network component representing a block of information encoded in a protocol and transmitted through the inter-network, the method comprising:

communicating the network component to the first node from a second node via the inter-network;

determining an identifier of the network component;

validating the identifier, validating the identifier further including determining a range for the identifier, a wrap count for the identifier, and an age limit for the identifier;

determining whether the network component was exactly one of (1) forwarded in its entirety by the second node to the first node and (2) forwarded in the form of the identifier by the second node to the first node.

13. The method of claim 12, further comprising:

if the network component was forwarded in its entirety, recursively validating one or more subcomponents of the network component.

14. The method of claim 13, wherein recursively validating the one or more subcomponents further includes validating a format for each of the plurality of subcomponents.

15. The method of claim 14, wherein recursively validating the one or more subcomponents further includes validating a syntax for each of the plurality of subcomponents.

16. The method of claim 15, wherein the syntax is at least partially specified by the network protocol.

17. The method claim 15, further comprising:

if a subcomponent from the plurality of subcomponents is invalid, indicating invalidity of the subcomponent to a security daemon in the network protocol.

18. The method of claim 14, further comprising determining if the network component has been retransmitted.

19. The method of claim 15, further comprising:

upon recursively validating the one or more subcomponents, resetting an aging time for the network component.

20. The method of claim 16, further comprising:

upon recursively validating the one or more subcomponents, updating a wrap around processing of the sequential identifier.

21. The method of claim 12, wherein the sequential identifier is monotonically increasing, modulo a wrap around limit for the subcomponent.

22. The method of claim 13, wherein the network protocol is an EGP.

23. The method of claim 22, wherein the EGP is a path vector protocol.

24. The method of claim 23, wherein the path vector protocol is a version of BGP.

25. The method of claim 13, wherein the network protocol is a link state protocol.

26. The method of claim 13, wherein the link state protocol is OSPF.

27. The method of claim 13, wherein the link state protocol is IS-IS.

28. A network component resident on an internetwork, the network component representing a common message transmitted in the internetwork via a communications protocol, the network component comprising:

a plurality of subcomponents arranged in a recursive hierarchy;

an identifier for each subcomponent of the plurality of subcomponents, such that for each subcomponent, the identifier is monotonically increasing for each transmission of each subcomponent, modulo a wrap around limit, wherein the wrap around limit indicates a maximum possible value of the identifier;

a transmission period for each respective subcomponent of the plurality of subcomponents, the transmission period designating a interval for retranslating the subcomponent in the internetwork, such that the respective subcomponent has transmission period less than or equal to a transmission period of one or more parent subcomponents from the plurality of subcomponents;

wherein one or more nodes in the internetwork are operative to validate the plurality of subcomponents by reference to the identifier and wrap around limit of each of the plurality of subcomponents, and the one or mode nodes are operative to increment the identifier of each of the plurality of subcomponents upon retransmission.

29. The network component of claim 28, further including an aging limit, such that the one or more nodes are operative to reset the identifier if a current time exceeds or equals the aging limit.

30. The network component of claim 28, wherein the communications protocol is an EGP.

31. The network component of claim 30, wherein the EGP is a path vector protocol.

32. The network component of claim 31, wherein the path vector protocol is BGP.

33. The network component of claim 29, wherein the communications protocol is a link state protocol.

34. The network component of claim 33, wherein the link state protocol is OSPF.

35. The network component of claim 34, wherein the link state protocol is IS-IS.

36. The network component of claim 29, wherein the one or more nodes are operative to reset an aging metric for each of the plurality of network components.

37. A packet transmitted in an inter-network, the packet comprising:

a plurality of component blocks in the packet arranged in a recursive hierarchy;

a first component block in the recursive hierarchy, the first component block including

a first field indicating a rank of the first network component in the recursive hierarchy,

a second field including a unique global identifier for the first component;

wherein the first network component substitutes for a first data pattern which has previously traversed the inter-network, such that the first network component is substantially shorter than the first data pattern.

38. The packet of claim 37, wherein the first data pattern encodes a message in an inter-network protocol.

39. The packet of claim 38, wherein the inter-network protocol is a link state protocol.

40. The packet of claim 39, wherein the link state protocol is IS-IS.

41. The packet of claim 39, wherein the link state protocol is a Shortest Path First protocol.

42. The packet of claim 41, wherein the link state protocol is an Open Shortest Path First protocol.

43. The packet of claim 38, wherein the inter-network protocol is a path vector protocol.

44. The packet of claim 38, wherein the inter-network protocol is a distance vector protocol.

45. The packet of claim 37, wherein the first data pattern encodes a series of parameters which appear frequently in packet headers communicated in the inter-network.

46. The packet of claim 37, further comprising:

a second component in the recursive hierarchy, the second component embedded in the first component, the second component substituting for a second data pattern which has previously traversed the inter-network.

47. The packet of claim 46 further comprising:a third field indicating a rank of the second network component in the recursive hierarchy,
a fourth field including a unique global identifier for the second component.

48. The packet of claim 47, wherein the rank of the second network component is lower than a rank of the first network component.

49. A method of transmitting a packet in an inter-network, the packet including a plurality of components, each of the plurality of components comprising a block of packet information, the method comprising:
at a first peer in the inter-network, receiving the packet:
identifying a first component in the plurality of components, wherein the first component is encoded in a default format, such that the first peer is operative to decipher the default format, identifying the default format further including identifying a global format identifier for the default format, wherein the global format identifier for the default format is embedded in the first component;
processing the first component at the first peer by reference to the default format;
determining a second format encoded by the first component, such that the second format was not previously stored in the first peer;
identifying a second component from the plurality of components, the second component recursively embedded in the first component, the second component compressing a block of network information frequently repeated in the inter-network, identifying the second component further including identifying a global format identifier for the second format, wherein the global format identifier for the second format is embedded in the second component.
decompressing the second component at the first peer by reference to the second format.

50. The method of claim 49, wherein the first and second peers are located in separate autonomous systems.

51. The method of claim 50, wherein the first and second peers are in communication via an Exterior Gateway Protocol.

52. The method of claim 51, wherein the Exterior Gateway Protocol is Border Gateway Protocol.

53. The method of claim 49, wherein the first and second peers are in a single autonomous system.

54. The method of claim 53, wherein the first and second peers are in communication via an Interior Gateway Protocol.

55. The method of claim 49, wherein the first and second peers are in communication via a distance vector protocol.

56. The method of claim 49, wherein the first and second peers are in communication via a link state protocol.

57. The method of claim 49, wherein the first and second peers are in communication over one of the group consisting of RIP, OSPF, ISIS.

58. The method of claim 49, further comprising:

assigning a unique identifier for the second network component.

59. The method of claim 58, wherein the unique identifier is monotonically increasing.

60. The method of claim 59, further comprising:

substituting the unique identifier of the second network component for the second network component in subsequent transmissions in the inter-network.

61. The method of claim 60, wherein the identifier of the second network component is significantly shorter the second network component itself.

62. The method of claim 49, wherein the block of network information includes a parameters frequently transmitted in packet headers through the inter-network.

63. A method of transmitting network information in a network, the method comprising:

identifying a pattern of network data frequently repeated within packets traversing the network;

generating a packet component to substitute for the packet of network data, generating the packet component including generating a unique, monotonically increasing identifier for the packet component;

transmitting the packet component embedded in a packet in the inter-network, wherein the packet component substitutes for the pattern of network data;

in place of the packet component, subsequently transmitting only the unique identifier to substitute for the pattern of network data, wherein the unique identifier is substantially shorter than the packet component.

64. The method of claim 63, wherein the network is a local area network.

65. The method of claim 63, wherein the network is an autonomous system.

66. The method of claim 63, wherein the network is an inter-network.

67. The method of claim 63, wherein the pattern of network data includes routing information.

68. The method of claim 67, wherein the routing information includes parameters in a routing protocol.

69. The method of claim 68, wherein the routing protocol is a link state protocol.

70. The method of claim 68, wherein the routing protocol is a distance vector protocol.

71. The method of claim 68, wherein the routing protocol is a path vector protocol.

72. The method of claim 63, wherein the pattern of network data includes information from a network security application.

73. The method of claim 72, wherein the network security application is a firewall.

74. The method of claim 72, wherein the network security application is a virtual private network (VPN) application.

75. The method of claim 38, wherein the VPN application is an IPSec application.

76. The method of claim 72, wherein the network security application is a Secure Socket Layer application.

77. The method of claim 63, wherein the pattern of network data includes information from a network monitoring application.

78. The method of claim 77, wherein the network monitoring application is based on Simple Network Monitoring Protocol.

79. The method of claim 63, wherein the pattern of network data includes information encoded in a communications protocol.

80. The method of claim 79, wherein the communications protocol is Simple Object Access Protocol.

81. The method of claim 79, wherein the communications protocol is a Common Object Request Broker Application.

82 . The method of claim 63, wherein the pattern of network data is encoded in XML.